ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Secured Way to Provide Privacy for User Location in Geo Social Applications

Mallela Narasimha Rao
M.Tech Student,
Department of CSE,
Loyola Institute of Technology and Management.

Y. Suresh
Assistant Professor,
Department of CSE,
Loyola Institute of Technology and Management.

N.Vijay Kumar
Professor & HOD,
Department of CSE,
Loyola Institute of Technology and Management.

Abstract:

Using geosocial applications, such as FourSquare, millions of people interact with their surroundings through their friends and their recommendations. Without adequate privacy protection, however, these systems can be easily misused, for example, to track users or target them for home invasion. In this paper, we introduce LocX, a novel alternative that provides significantly improved location privacy without adding uncertainty into query results or relying on strong assumptions about server security. Our key insight is to apply secure user-specific, distance-preserving coordinate transformations to all location data shared with the server.

The friends of a user share this user's secrets so they can apply the same transformation. This allows all location queries to be evaluated correctly by the server, but our privacy mechanisms guarantee that servers are unable to see or infer the actual location data from the transformed data or from the data access. We show that LocX provides privacy even against a powerful adversary model, and we use prototype measurements to show that it provides privacy with very little performance overhead, making it suitable for today's mobile devices.

Keywords:

FourSquare, GeoSocial, LocX, LBSA'S, Privacy

1. INTRODUCTION:

With billions in downloads and annual revenue, smartphone applications offered by Apple iTunes and Android are quickly becoming the dominant computing platform for today's user applications. Within these markets, a new wave of geo-social applications is fully exploiting GPS location services to provide a "social" interface to the physical world.

Examples of popular social applications include social rendezvous local friend recommendations for dining and shopping as well as collaborative network services and games.The explosive popularity of mobile social networks such as SCVNGR and FourSquare (3 million new users in 1 year) likely indicate that in the future, social recommendations will be our primary source of information about our surroundings. Unfortunately, this new functionality comes with significantly increased risks to personal privacy. Geo-social applications operate on fine-grain, time-stamped location information.

For current services with minimal privacy mechanisms, this data can be used to infer a user's detailed activities, or to track and predict the user's daily movements. In fact, there are numerous real world examples where the unauthorized use of location information has been misused for economic gain, physical stalking, and to gather legal evidence. Even more disturbing, it seems that less than a week after Facebook turned on their popular "Places" feature for tracking users' locations, such location data was already used by thieves to plan home invasions. Clearly, mobile social networks of tomorrow require stronger privacy properties than the opento-all policies available today.

2. EXISTING SYSTEM:

Existing systems have mainly taken three approaches to improving user privacy in geosocial systems:

• Introducing uncertainty or error into location data.

•Relying on trusted servers or intermediaries to apply anonymization to user identities and private data.

•Relying on heavy-weight cryptographic or private information retrieval (PIR) techniques.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Fig 1: A basic design.

None of them, however, have proven successful on current application platforms. Techniques using the first approach fall short because they require both users and application providers to introduce uncertainty into their data, which degrades the quality of application results returned to the user.

In this approach, there is a fundamental tradeoff between the amount of error introduced into the time or location domain, and the amount of privacy granted to the user. Users dislike the loss of accuracy in results, and application providers have a natural disincentive to hide user data from themselves, which reduces their ability to monetize the data.

The second approach relies on the trusted proxies or servers in the system to protect user privacy. This is a risky assumption, since private data can be exposed by either software bugs or configuration errors at the trusted servers or by malicious administrators.

Finally, relying on heavy-weight cryptographic mechanisms to obtain provable privacy guarantees are too expensive to deploy on mobile devices and even on the servers in answering queries such as nearest neighbor and range queries.

DISADVANTAGES OF EXISTING SYSTEM:

•Location data privacy. The servers should not be able to view the content of data stored at a location.

• This new functionality comes with significantly increased risks to personal privacy.

3. PROPOSED SYSTEM:

In this paper, we propose LocX(short for location to index mapping), a novel approach to achieving user privacy while maintaining full accuracy in location-based social applications (LBSAs from here on ward). Our insight is that many services do not need to resolve distance-based queries between arbitrary pairs of users, but only between friends interested in each other's locations and data. Thus, we can partition location data based on users' social groups, and then perform transformations on the location coordinates before storing them on untrusted servers. A user knows the transformation keys of all her friends, allowing her to transform her query into the virtual coordinate system that her friends use. Our coordinate transformations preserve distance metrics, allowing an application server to perform both point and nearest-neighbor queries correctly on transformed data. However, the transformation is secure, in that transformed values cannot be easily associated with real-world locations without a secret, which is only available to the members of the social group. Finally, transformations are efficient, in that they incur minimal overhead on the LBSAs. This makes the applications built on LocX lightweight and suitable for running on today's mobile devices.

ADVANTAGES OF PROPOSED SYSTEM:

•Our goal is to support both query types in an efficient fashion, suitable for today's mobile devices.

• Flexibility to support point, circular range, and nearest-neighbor queries on location data.

•Strong location privacy. The servers processing the data (and the administrators of these servers) should not be able to learn the history of locations that a user has visited.

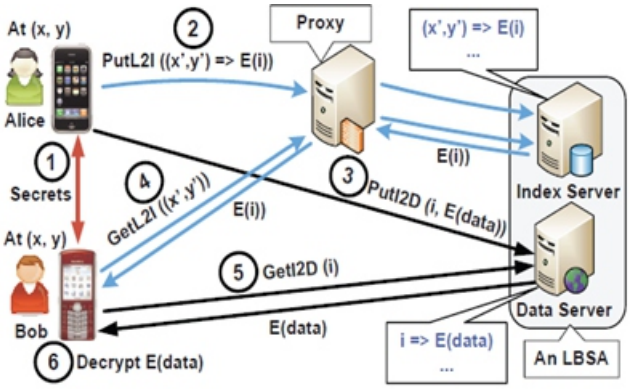

Fig 2: Design of LOCX.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

4. IMPLEMENTATION MAIN MODULES:

1.Locx module
2.Proxy server
3.Index server
4.Data Server

LOCX Module:

Loc X builds on top of the basic design, and introduces two new mechanisms to overcome its limitations. First, in Loc X, we split the mapping between the location and its data into two pairs: a mapping from the transformed location to an encrypted index (called L2I), and a mapping from the index to the encrypted location data (called I2D). This splitting helps in making our system efficient. Second, users store and retrieve the L2Is via untrusted proxies. This redirection of data via proxies, together with splitting, significantly improves privacy in LocX. For efficiency, I2Ds are not proxied, yet privacy is preserved (as explained later).

Proxying L2Is for location privacy:

Users store their L2Ison the index server via untrusted proxies. These proxies can be any of the following: Planet Lab nodes, corporate NAT sand email servers in a user's work places, a user's home and office desktops or laptops, or Tor [34] nodes. We only need a one-hop indirection between the user and the index server. These diverse types of proxies provide tremendous flexibility in proxying L2Is, thus a user can store her L2Is via different proxies without restricting herself to a single proxy.

Furthermore, compromising these proxies by an attacker does not break users' location privacy, as (a) the proxies also only see transformed location coordinates and hence do not learn the users' real locations, and (b) due to the noise added toL2Is (described later). To simplify the description, for now, we assume that the proxies are non-malicious and do not collude with the index server. But we will later describe our solution in detail to even defend against colluding, malicious proxies. With this high-level overview, we now describe our solution to store and query data on the servers in detail. We also explain the challenges we faced, and the tradeoffs we made in making our solution secure and efficient.

Storing L2I on the index server:

First consider storing L2I on the index server. This transformation preserves the distances between points1, so circular range and nearest neighbor queries for a friend's location data can be processed in the same way on transformed coordinates as on real-world coordinates. Then the user generates a random index (i) using her random number generator and encrypts it with her symmetric key to obtain at the transformed coordinate on the index server via a proxy. The L2I is small in size and is application independent, as it always contains the coordinates and an encrypted random index. Thus the over head due to proxying is very small.

Storing I2Ds on the data server:

The user can directly storeI2Ds (location data) on the data server. This is both secure and efficient.1) This is secure because the data server only sees the index stored by the user and the corresponding encrypted blob of data. In the worst case, the data server can link all the different indices to the same user device, and then link these indices to the retrieving user's device. But this only reveals that one user is interested in another user's data, but not any information about the location of the users, or the content of the I2Ds, or the real-world sites to which the data in the encrypted blob corresponds to.

2) The content of I2Dis application dependent. For example, a location-based video or photo sharing service might share multiple MBs of data at each location. Since this data is not proxied, LocX still maintains the efficiency of today's systems.

Mechanisms:

In this we use Locx Mechanisms is used in this project.
1) Alice and Bob exchange their secrets,
2) Alice generates and L2I and I2D from her review of the restaurant (at (x, y)), and stores the L2I on the index server via a proxy.
3) She then stores the I2D on the data server directly
4) Bob later visits the restaurant and fetches for L2Is from his friends by sending the transformed coordinates via a proxy.
5) He decrypts the L2I obtained and then queries for the corresponding I2D,
6) Finally Bob decrypts Alice's review.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

5 CONCLUSIONS:

This paper describes the design, prototype implementation, and evaluation of LocX, a system for building location-based social applications (LBSAs) while preserving user location privacy. LocX provides location privacy for users without injecting uncertainty or errors into the system, and does not rely on any trusted servers or components. LocX takes a novel approach to provide location privacy while maintaining overall system efficiency, by leveraging the social data-sharing property of the target applications. In LocX, users efficiently transform all their locations shared with the server and encrypt all location data stored on the server using inexpensive symmetric keys. Only friends with the right keys can query and decrypt a user's data. We introduce several mechanisms to achieve both privacy and efficiency in this process, and analyze their privacy properties.

REFERENCES:

[1] M. Motani, V. Srinivasan, and P. S. Nuggehalli, "Peoplenet:engineering a wireless virtual social network," in Proc. of MobiCom, 2005.

[2] M. Hendrickson, "The state of location-based social networking," 2008.

[3] P. Mohan, V. N. Padmanabhan, and R. Ramjee, "Nericell: rich monitoring of road and traffic conditions using mobile smartphones," in Proc. of SenSys, 2008.

[4] G. Ananthanarayanan, V. N. Padmanabhan, L. Ravindranath, and C. A. Thekkath, "Combine: leveraging the power of wireless peers through collaborative downloading," in Proc. of MobiSys, 2007.

[5] M. Siegler, "Foodspotting is a location-based game that will make your mouth water," http://techcrunch.com/2010/03/04/foodspotting/.

[6] http://www.scvngr.com.

[7] B. Schilit, J. Hong, and M. Gruteser, "Wireless location privacy protection," Computer, vol. 36, no. 12, pp. 135–137, 2003.

[8] F. Grace, "Stalker Victims Should Check For GPS," Feb. 2003, www.cbsnews.com.

[9] DailyNews, "How cell phone helped cops nail key murder suspect secret 'pings' that gave bouncer away," Mar. 2006.

[10] "Police: Thieves robbed homes based on facebook,social media sites," WMUR News, September 2010,http://www.wmur.com/r/24943582/detail.html.

[11] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in Proc. of Mobisys, 2003.

[12] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: A privacyaware location-based database server," in ICDE, 2007.

[13] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in Proc. of ICDCS, 2005.

[14] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless lans," in Proc. of MobiSys, 2007.

[15] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," TKDE, 2007.

[16] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: anonymizers are not necessary," in SIGMOD Conference, 2008.

[17] S. Papadopoulos, S. Bakiras, and D. Papadias, "Nearest neighbor search with strong location privacy," PVLDB, 2010.

[18] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location privacy via private proximity testing," in Proc. of NDSS, 2011.

[19] G. Zhong, I. Goldberg, and U. Hengartner, "Louis, lester and pierre: Three protocols for location privacy," in Proc. of PET, 2007.